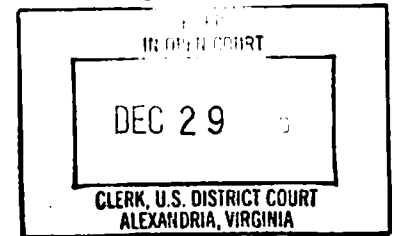


UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

JAMES E. HANCOCK,
a/k/a "Pedro," "Pedro223"
Defendant.

Criminal No. 1:15-cr-172-4

STATEMENT OF FACTS

The United States and the defendant, James E. Hancock, agree that the following is true and that had this matter proceeded to trial, the United States would have proven the following facts beyond a reasonable doubt through admissible and credible evidence and testimony:

1. In about September 2014, law enforcement agents of the Federal Bureau of Investigation learned of a website ("Website A") operated by a group of individuals, including one individual in the Eastern District of Virginia. The object and purpose of Website A was to entice children to engage in sexual activity through live web camera videos. Upgraded members of Website A had access to private portions of the website and were able to view and download child pornography from the website, including child pornography that they had produced using web-camera videos of children who had been lured to the site. Website A was shut down in September 2014 by its members due to security concerns, and in about October 2014, members of Website A started Website B, which had substantially the same purpose and functionality as Website A.

2. Members of Website A and Website B scoured social media and video-sharing sites popular with children and young teenagers, such as YouTube, to try to meet them and lure them to Website A and Website B. In some instances, this was done by members who pretended to be minors themselves, and in other instances, this was accomplished by custom-designed automated programs.

3. Members engaged in “linking” to lure minor victims by generating and posting a link which—if clicked—took the minor victim into a chat room on Website A or Website B that appeared to be a private one-on-one chat. In reality, other upgraded members who stayed in the general “lounge” area could receive notifications that a minor victim had entered a chat room. This notification provided the minor victim’s screen name for the website, their room location, and their geographic location by city and state. Upgraded members waiting in the “lounge” could then enter the room invisibly and watch the activity unannounced and unbeknownst to the minor victim.

4. After the original member invited the minor victim into the private chat (i.e. “linked” the minor), that member or other members chatted with the minor victim on Website A or Website B, and often used deception to persuade, induce, entice, and coerce the minor victim into producing and transmitting sexually explicit videos of themselves. While text-chatting with the minor in real-time, some members posed as minors themselves and simultaneously streamed pre-recorded video of child pornography captured by web-camera (these videos were called “loops”) to trick the minor victim into engaging in sexually explicit behavior on web camera as well. The unwitting minor victim did not know that video that they transmitted on the site was

being watched in real-time by multiple upgraded users of the sites or was being recorded and would be available for select users to download and view later.

5. The foregoing methods were not the exclusive means used to persuade, induce, entice and coerce minors to engage in sexually explicit webcam videos. Members also chatted openly with minors in rooms, meaning that the members would neither pretend to be minors nor hide the presence of others in a room.

6. Website A tracked upgraded members' contributions to the website, ranking for example, the most prolific at "chatting," "looping," and "linking." Members also referred to "wins" as successfully linking and luring a minor victim into engaging in sexually explicit conduct.

7. To date, the FBI has identified more than 240 minor victims, although it is estimated that the conspiracy involved more than a thousand child victims in the United States and abroad. At least 137 of these victims engaged in sexually explicit conduct on web camera on Website A or Website B. The FBI has identified more than 65,000 videos associated with Website A and Website B. To date, approximately 9,000 of these videos have been identified as child pornography, with many other videos being sexually suggestive.

8. Defendant JAMES E. HANCOCK was a member of Website A and Website B and used the following online names: "Pedro" and "Pedro223."

9. Defendant JAMES E. HANCOCK became a member and logged into Website A and Website B with knowledge that the purpose and objectives of the websites were to convince or trick children into engaging in sexually explicit conduct online and with intent to engage in a conspiracy to distribute and receive child pornography.

10. For example, on or about April 23, 2014, defendant JAMES E. HANCOCK logged into Website A, used the username “pedro,” and joined a room in which Website A members were persuading Minor A, an identified female who was under 18 years old, to engage in sexually explicit conduct, including digital penetration and masturbation with a brush, over live video web camera.

11. At the end of this chat, Minor A left the room for a new room that was password protected by an administrator of Website A. Defendant HANCOCK, asked for a password to the “party” and entered a room called “PARTY NOW,” in which members were persuading Minor A to engage in sexually explicit conduct, including masturbation with objects. After HANCOCK entered the room, Minor A showed her breasts and HANCOCK replied, “beautiful [Minor A] thank you.” After Minor A left the room, a member with the username “sean” remarked, “she is awesome.” HANCOCK replied “agreed sean.”

12. On other occasions, in or about April and May 2014, defendant JAMES E. HANCOCK logged into Website A for the purpose of and with intent to engage in a conspiracy to distribute and receive child pornography. Defendant HANCOCK occasionally chatted but primarily returned to observe the child pornography for sexual gratification. For example, on or about April 27, 2014, HANCOCK logged into Website A and joined a room in which members were persuading Minor N, an identified minor under the age of 18, to engage in sexually explicit conduct over live video web camera. Minor N, who purported to be 12 years old, exposed her genital and pubic area.

13. The defendant JAMES E. HANCOCK viewed minors engaged in sexually explicit conduct on Website A.

14. After Website A was shut down, defendant JAMES E. HANCOCK learned about the new website, Website B. Defendant HANCOCK logged into it from his home (IP address 216.212.224.95) on October 17, 2014 and place of business (IP Address 209.37.15.57) on October 23, 2014 in Thomasville, Georgia. Defendant HANCOCK logged in on those occasions for the purpose of and with intent to engage in a conspiracy to distribute and receive child pornography, but the website was not fully functional.

15. On February 4, 2015, FBI agents executed a search warrant at defendant JAMES E. HANCOCK's residence and place of business. After being informed of his *Miranda* rights, defendant HANCOCK admitted during a voluntary interview that he had special access and could view child pornography on Website A, that he saw on Website A nudity involving children younger than 18, and that he returned to the site for "titillation." HANCOCK tried to exploit features of Website A to gain more access to rooms that he did not have permission to enter and view live web camera feed that he did not have permission to view. HANCOCK admitted to accessing Website B but said it was not fully functional.

16. Defendant JAMES E. HANCOCK stated that he generally prefers to watch live web camera streams rather than download files containing child pornography to his computer. Nevertheless, he admitted to having used UseNet, an online forum, to download child pornography.

17. A forensic examination of defendant JAMES E. HANCOCK's computers revealed files and browser activity relating to Website A as well as deleted URLs relating to Websites A and B. It also revealed that HANCOCK used the name "pedro223" to access a Usenet newsgroup reader program "XNews.exe." Finally, it revealed that in or about October

2014, in the Middle District of Georgia, Hancock downloaded to an “mbx” email-type file container approximately 40 child pornography files, including images depicting a prepubescent female being anally penetrated by an adult male, an image depicting the genital and pubic area of a prepubescent female, and a prepubescent child performing oral sex on an adult male.

18. In addition to Websites A and B, defendant JAMES E. HANCOCK visited two other websites which had substantially the same purpose as Websites A and B. He joined these websites with the intent to view and gain access to child pornography.

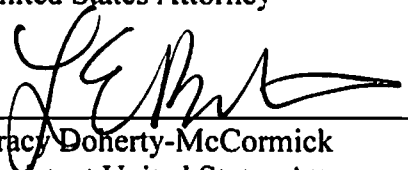
19. The Statement of Facts includes those facts necessary to support the defendant’s guilty plea. It does not include each and every fact known to the defendant or to the government and it is not intended to be a full enumeration of all of the facts surrounding the defendant’s case.

20. The actions of the defendant, as recounted above, were in all respects knowing and intentional, and were not committed by mistake, accident or other innocent reason.

Respectfully submitted,

Dana J. Boente
United States Attorney

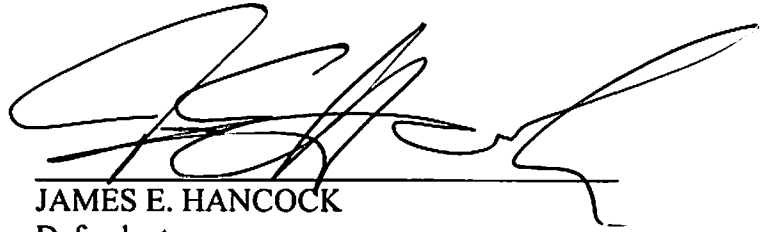
By: _____


Tracy Doherty-McCormick
Assistant United States Attorney
Lauren Britsch
Special Assistant United States Attorney (LT)

DEFENDANT'S SIGNATURE

After consulting with my attorney, I hereby stipulate that the above Statement of Facts is true and accurate and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

Date: 12/29/2015

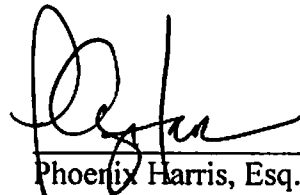


JAMES E. HANCOCK
Defendant

DEFENSE COUNSEL'S SIGNATURE

I am JAMES E. HANCOCK's attorney. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

Date: 12/29/15



Phoenix Harris, Esq.
Counsel for the Defendant